

## Vorwort

Neu strukturiert und international ausgerichtet - so lassen sich kurz und knapp die Veränderungen innerhalb der neuen Version des IT-Grundschutzhandbuchs zusammenfassen.

Was können Sie davon erwarten? Eine Menge! Durch den neuen ISO-Standard 27001 ist es ab jetzt möglich, auch Managementsysteme für Informationssicherheit zu zertifizieren. Damit das IT-Grundschutz-Zertifikat auch diese internationale Norm erfüllt, hat das BSI die IT-Grundschutz-Vorgehensweise, das Zertifizierungsschema und die IT-Grundschutz-Kataloge überarbeitet. Stärker als bisher steht das ganzheitliche Risikomanagement im Fokus. So wird Informationssicherheit ausgehend von den Geschäftsprozessen umgesetzt.

Obwohl Neues kommt, bleibt Bewährtes bestehen: Nach wie vor enthalten sind Standard-Sicherheitsmaßnahmen und Hinweise für die Umsetzung des IT-Grundschutzes in einer Organisation. Einzelne Bausteine helfen das Sicherheitsniveau von IT-Umgebungen zu erhöhen und vereinfachen die Erstellung von IT-Sicherheitskonzepten. Die Maßnahmen orientieren sich dabei an einem Schutzbedarf, der für die meisten IT-Einsatzumgebungen zutrifft. Sie bauen auf der IT-Grundschutz-Vorgehensweise auf, die es ab jetzt in einem separaten Dokument gibt. Zahlreiche Hilfsmittel wie das GSTOOL runden die IT-Grundschutz-Methodik und die IT-Grundschutz-Kataloge ab.

Mit dieser überarbeiteten Version der IT-Grundschutz-Kataloge ist es dem BSI gelungen, erneut einen wichtigen Beitrag für mehr Sicherheit in der Informationstechnik zu leisten. Denn um Sicherheitsdefizite zu ermitteln und passende Maßnahmen zu bestimmen, sind keine aufwändigen Analysen mehr erforderlich, sondern nur noch ein Soll-Ist-Abgleich der Maßnahmen. Um mit dem Entwicklungstempo der Informationstechnik auch zukünftig Schritt halten zu können, werden die IT-Grundschutz-Kataloge auch weiterhin einmal jährlich aktualisiert. Bedanken möchte ich mich für Ihre zahlreichen Verbesserungsvorschläge - für die in der Vergangenheit und auch für die in der Zukunft!

Bonn, im November 2005



Dr. Udo Helmbrecht, Präsident des BSI

**Hinweis:**

Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

## Dankesworte

Aufgrund der jährlichen Bedarfsabfrage bei registrierten Anwendern werden die IT-Grundschutz-Kataloge bedarfsorientiert weiterentwickelt. Für die Mitarbeit bei der Weiterentwicklung des IT-Grundschutzes und die engagierte Unterstützung bei der Fortschreibung der 7. Ergänzungslieferung der IT-Grundschutz-Kataloge wird an dieser Stelle folgenden Beteiligten gedankt:

- |   |  |
|---|--|
| - Gesamtkoordination  | Frau Isabel Münch, BSI   |
| - Redaktionelle Bearbeitung und Hotline                             | Frau Elke Cäsar, BSI<br>Frau Gabriele Scheer-Gumm, BSI<br>Frau Petra Simons-Felwor, BSI  |
| - Baustein B 1.13 IT-Sicherheitssensibilisierung und -schulung      | Frau Isabel Münch, BSI<br>Frau Dr. Lydia Tsintsifa, BSI  |
| - Baustein B 3.209 Client unter Windows XP                          | Herr Albert Vetter, Eurosec<br>Herr Thomas Caspers, BSI<br>Frau Dr. Lydia Tsintsifa, BSI   |
| - Baustein B 2.10 Mobiler Arbeitsplatz                              | Frau Isabel Münch, BSI<br>Herr Frank Weber, BSI  |
| - Baustein B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume | Frau Isabel Münch, BSI<br>Herr Frank Weber, BSI  |
| - Überarbeitung Baustein B 1.0 IT-Sicherheitsmanagement             | Frau Isabel Münch, BSI<br>Frau Angelika Jaschob, BSI<br>Herr Dr. Harald Niggemann, BSI<br>Frau Dr. Lydia Tsintsifa, BSI<br>Frau Steffi Botzelmann, BSI |
| - Überarbeitung Baustein B 1.1 Organisation                         | Frau Gabriele Scheer-Gumm, BSI   |
| - Überarbeitung Baustein B 1.2 Personal                             | Frau Gabriele Scheer-Gumm, BSI   |
| - Überarbeitung Baustein B 3.101 Allgemeiner Server                 | Herr Thomas Häberlen, BSI<br>Herr Holger Schildt<br>Frau Dr. Lydia Tsintsifa, BSI  |
| - Überarbeitung Baustein B 3.201 Allgemeiner Client                 | Herr Thomas Häberlen, BSI<br>Herr Holger Schildt<br>Frau Dr. Lydia Tsintsifa, BSI  |
| - Überarbeitung Baustein B 3.203 Laptop                             | Hr. Gerhard Weck, INFODAS<br>Frau Isabel Münch, BSI  |
| - Qualitätssicherung  | Hr. Gerhard Weck, INFODAS<br>Herr Marcel Birkner, BSI  |

Neben der Aktualisierung und Überarbeitung von Bausteinen wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst. Auch hier sei den Mitwirkenden gedankt.

Darüber hinaus sei allen gedankt, die sich durch konstruktive Kritik und praktische Verbesserungsvorschläge an der Verbesserung des IT-Grundschutzes und der IT-Grundschutz-Kataloge beteiligt haben.

Bei der Fortschreibung und Weiterentwicklung vorhergehender Versionen des IT-Grundschutzhandbuchs haben die nachfolgend aufgezählten Personen und Institutionen mitgewirkt. Auch ihnen sei hiermit Dank ausgesprochen:

- Atos Origin  
Herr Herbert Blaauw, Herr Matthias Mönter  
Herr Götz, Herr Jaster, Herr Pohl
- ConSecur GmbH  
Herr Nedon, Herr Eckardt
- Daimler-Benz AG  
Herr Heinle, Hr. Schlette
- Europäische Kommission  
GD Informationsgesellschaft  
Herr Achim Klabunde
- EUROSEC GmbH  
Herr Fünfroeken  
Herr Dr. Zieschang
- Evangelische Kirche von Westfalen,  
Das Landeskirchenamt  
Herr Huget
- Flughafen Düsseldorf GmbH  
Herr Andreas Peters
- GUIDE SHARE EUROPE  
Arbeitskreis "DATENSCHUTZ und  
DATENSICHERHEIT"
- Henkel KGaA  
Herr Rhefus
- HiSolutions Software GmbH  
Herr Alexander Geschonneck
- INFODAS  
Herr Dr. Weck
- Ingenieurbüro Mink
- Innenministerium des Landes  
Schleswig-Holstein  
Herr Kuhr
- Landesbeauftragter für den Datenschutz  
Saarland  
Herr Simon
- Fa. Novell
- Fa. Oracle
- Röhm GmbH Chemische Fabrik  
Datenschutzbeauftragter  
Herr Güldemeister
- T-Systems International GmbH  
Herr Stephan Hüttinger, Herr Torsten Kullich,  
Herr Klaus Müller, Herr Stefan Morkovsky,  
Herr Axel Nennker
- Universität GH Essen, FB Wirtschaft-  
informatik  
Herr Prof. Dr. Voßbein
- Universitätsklinikum der TU Dresden  
Klinik für Orthopädie  
Herr Frank Heyne
- Verband der Chemischen Industrie e. V.
- VZM GmbH  
Herr Bruno Hecht, Herr Werner Metterhausen,  
Herr Rainer von zur Mühlen
- Zentrale Datenverarbeitungsstelle für das  
Saarland  
Herr Müller

Folgende Autoren haben durch die Erstellung von Bausteinen ihr Fachwissen in die IT-Grundschutz-Kataloge einfließen lassen. Ihnen gebührt besonderer Dank, da ihr Engagement die Entstehung und Weiterentwicklung der IT-Grundschutz-Kataloge erst ermöglicht hat.

Bundesministerium des Innern: Herr Jörg-Udo Aden, Herr André Reisen, Herr Manfred Kramer

Bundesministerium für Bildung und Wissenschaft: Herr Frank Stefan Stumm

Bundesamt für Sicherheit in der Informationstechnik: Herr Rainer Belz, Herr Thomas Biere, Herr Björn Dehms, Herr Uwe Dornseifer, Herr Günther Ennen, Herr Olaf Erber, Herr Frank W. Felzmann, Herr Michael Förtsch, Herr Dr. Kai Fuhrberg, Herr Dr. Dirk Häger, Herr Dr. Hartmut Isselhorst, Herr Harald Kelter, Herr Kurt Kliner, Herr Dr. Christian Mrugalla, Frau Isabel Münch, Herr Robert Rasten, Frau Martina Rohde, Herr Michael Ruck, Herr Fabian Schelo, Herr Heiner Schorn, Herr Dr. Ernst Schulte-Geers, Herr Carsten Schulz, Herr Bernd Schweda, Frau Katja Vogel, Herr Frank Weber, Herr Helmut Weisskopf, Herr Dr. Stefan Wolf

## Inhaltsverzeichnis - IT-Grundschutz-Kataloge

### 0 Allgemeines

Vorwort des Präsidenten  
Dankesworte  
Inhaltsverzeichnis  
Neues in Version 2005 der IT-Grundschutz-Kataloge

### 1 IT-Grundschutz - Basis für IT-Sicherheit

- 1.1 Warum ist IT-Sicherheit wichtig?
- 1.2 IT-Grundschutz: Ziel, Idee und Konzeption
- 1.3 Aufbau der IT-Grundschutz-Kataloge
- 1.4 Anwendungsweisen der IT-Grundschutzkataloge

### 2 Schichtenmodell und Modellierung

- 2.1 Modellierung nach IT-Grundschutz
- 2.2 Zuordnung anhand Schichtenmodell

### 3 Rollen

### 4 Glossar

### 5 Index

## Bausteinkataloge

### Schicht 1 Übergreifende Aspekte

- B 1.0 IT-Sicherheitsmanagement
- B 1.1 Organisation
- B 1.2 Personal
- B 1.3 Notfallvorsorge-Konzept
- B 1.4 Datensicherungskonzept
- B 1.5 Datenschutz
- B 1.6 Computer-Virenschutzkonzept
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.9 Hard- und Software-Management
- B 1.10 Standardsoftware
- B 1.11 Outsourcing
- B 1.12 Archivierung
- B 1.13 IT-Sicherheitssensibilisierung und -schulung

**Schicht 2    Infrastruktur**

- B 2.1 Gebäude
- B 2.2 Verkabelung
- B 2.3 Büroraum
- B 2.4 Serverraum
- B 2.5 Datenträgerarchiv
- B 2.6 Raum für technische Infrastruktur
- B 2.7 Schutzschränke
- B 2.8 Häuslicher Arbeitsplatz
- B 2.9 Rechenzentrum
- B 2.10 Mobiler Arbeitsplatz
- B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume

**Schicht 3    IT-Systeme**

- B 3.101 Allgemeiner Server
- B 3.102 Server unter Unix
- B 3.103 Server unter Windows NT
- B 3.104 Server unter Novell Netware 3.x
- B 3.105 Server unter Novell Netware Version 4.x
- B 3.106 Server unter Windows 2000
- B 3.107 S/390- und zSeries-Mainframe
  
- B 3.201 Allgemeiner Client
- B 3.202 Allgemeines nicht vernetztes IT-System
- B 3.203 Laptop
- B 3.204 Client unter Unix
- B 3.205 Client unter Windows NT
- B 3.206 Client unter Windows 95
- B 3.207 Client unter Windows 2000
- B 3.208 Internet-PC
- B 3.209 Client unter Windows XP
  
- B 3.301 Sicherheitsgateway (Firewall)
- B 3.302 Router und Switches
  
- B 3.401 TK-Anlage
- B 3.402 Faxgerät
- B 3.403 Anrufbeantworter
- B 3.404 Mobiltelefon
- B 3.405 PDA

**Schicht 4    Netze**

- B 4.1 Heterogene Netze
- B 4.2 Netz- und Systemmanagement
- B 4.3 Modem
- B 4.4 Remote Access
- B 4.5 LAN-Anbindung eines IT-Systems über ISDN

## **Schicht 5 IT-Anwendungen**

- B 5.1 Peer-to-Peer-Dienste,
- B 5.2 Datenträgeraustausch
- B 5.3 E-Mail
- B 5.4 Webserver
- B 5.5 Lotus Notes
- B 5.6 Faxserver
- B 5.7 Datenbanken
- B 5.8 Telearbeit
- B 5.9 Novell eDirectory
- B 5.10 Internet Information Server
- B 5.11 Apache Webserver
- B 5.12 Exchange 2000 / Outlook 2000

## **Gefährdungskataloge**

- G 1 Höhere Gewalt
- G 2 Organisatorische Mängel
- G 3 Menschliche Fehlhandlungen
- G 4 Technisches Versagen
- G 5 Vorsätzliche Handlungen

## **Maßnahmenkataloge**

- M 1 Infrastruktur
- M 2 Organisation
- M 3 Personal
- M 4 Hardware / Software
- M 5 Kommunikation
- M 6 Notfallvorsorge



## Neues in Version 2005 der IT-Grundschutz-Kataloge

### Umstrukturierung des IT-Grundschutzhandbuchs

Das IT-Grundschutzhandbuch ist mit dieser Ausgabe in verschiedenen Bereichen umstrukturiert worden. Am auffälligsten ist hierbei, dass die Beschreibung der Grundschutz-Vorgehensweise und die IT-Grundschutz-Kataloge getrennt wurden. Außerdem wurden noch eine Vielzahl kleinerer und größerer Änderungen aufgrund der Diskussionen mit Anwendern im In- und Ausland vorgenommen. So wurden beispielsweise zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst.

Die Nummerierung bestehender Gefährdungen und Maßnahmen blieb erhalten, so dass ein auf Basis der IT-Grundschutz-Kataloge erstelltes Sicherheitskonzept fortgeschrieben werden kann.

### Internationale Entwicklung

In der internationalen Standardisierungsorganisation ISO wurden nicht nur die Standards ISO 13335 und ISO 17799 überarbeitet, sondern auch die Möglichkeit eröffnet, Informationssicherheitsmanagement-Systeme zu zertifizieren. Hierfür wurde der Standard ISO 27001 als Grundlage für die Zertifizierung verabschiedet.

Das BSI hat 2002 die Zertifizierung von Geschäftsprozessen und IT-Verbünden auf Basis von IT-Grundschutz etabliert. Allen IT-Grundschutz-Anwendern soll es möglich sein, sich auch weiterhin die sorgfältige Umsetzung von IT-Grundschutz mit einem IT-Grundschutz-Zertifikat bestätigen zu lassen. Damit das IT-Grundschutz-Zertifikat aber auch die internationale Norm ISO 27001 mit abdeckt, wurden sowohl die IT-Grundschutz-Vorgehensweise, das Zertifizierungsschema und die IT-Grundschutz-Kataloge angepasst.

Eine IT-Grundschutz-Zertifizierung (oder jetzt: ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz) umfasst sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz. Sie beinhaltet gleichzeitig eine ISO-Zertifizierung nach ISO 27001, ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung. Die Lizenzierung von IT-Grundschutz-Auditoren wurde ebenfalls geändert, so dass vom BSI lizenzierte Auditoren alle Anforderungen erfüllen, die ISO an Auditoren für ein Informationssicherheitsmanagement-System stellt.

### BSI-Standards

Das BSI hat damit begonnen, eine Schriftenreihe mit Standards zu verschiedenen Bereichen der Informationssicherheit aufzubauen. Hierzu gehören auch die folgenden BSI-Standards:

BSI-Standard 100-1: Managementsysteme für Informationssicherheit

BSI-Standard 100-2: Vorgehensweise nach IT-Grundschutz

BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Darüber hinaus ist das Prüfungs- und Lizenzierungsschema für Auditoren im Dokument "ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz" beschrieben.

Außerdem wurde der Baustein 1.0 *IT-Sicherheitsmanagement* der IT-Grundschutz-Kataloge angepasst, um eine noch bessere Kompatibilität mit anderen internationalen Standards zu erreichen.

### Neuer Aufbau der IT-Grundschutz-Kataloge

Da die Beschreibung der IT-Grundschutz-Vorgehensweise in ein separates Dokument ausgelagert wurde, sind die einführenden Kapitel in die IT-Grundschutz-Kataloge gestrafft worden. Sie umfassen

jetzt im Wesentlichen neben einer Einführung einen Kurzüberblick über die Anwendungsweise der IT-Grundschutz-Kataloge und die Modellierungshinweise.

Darüber hinaus wurden die Grundschutz-Bausteine an das Schichtenmodell des IT-Grundschutzes angepasst, die Baustein-Beschreibungen aktualisiert sowie in eine einheitliche Form gebracht.

Die IT-Grundschutz-Bausteine basieren auf einem Schichtenmodell, das dazu dient,

- die Bausteine der IT-Grundschutz-Kataloge, gruppiert nach bestimmten Themen, einfacher auf einen komplexen IT-Verbund abbilden zu können und
- Redundanzen zu vermeiden, indem übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden.

Die einzelnen Schichten sind so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt sind. Schicht 1 betrifft Grundsatzfragen des IT-Einsatzes, Schicht 2 den Bereich Haus-technik, Schicht 3 die Ebene der Administratoren und IT-Benutzer, Schicht 4 die Netz- und Systemadministratoren und Schicht 5 schließlich die IT-Anwendungsverantwortlichen und -betreiber.

Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in resultierenden IT-Sicherheitskonzepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich tangiert werden.

Jeder Baustein ist einer Schicht zugeordnet. Diese Zuordnung spiegelt sich jetzt auch in der Gliederung der IT-Grundschutz-Kataloge wieder.

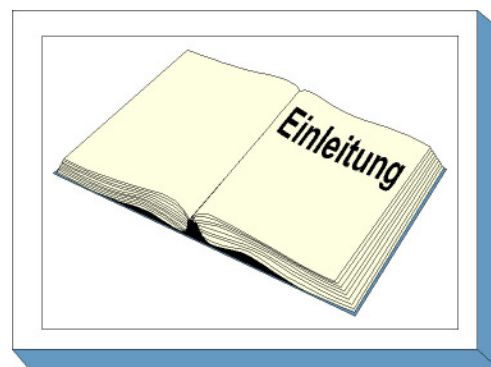
In jedem Baustein wird für das betrachtete Themengebiet vor der Aufzählung der umzusetzenden Maßnahmen eine Übersicht in Form eines "Lebenszyklus" gegeben. Hierin wird aufgezeigt, welche Maßnahmen in welcher Phase der Bearbeitung zu welchem Zweck ausgeführt werden sollen. Als Lebenszyklus-Phasen wurden Planung und Konzeption, Beschaffung (wo sinnvoll), Umsetzung, Betrieb, Aussonderung bzw. Außerbetriebnahme (soweit erforderlich) und Notfallvorsorge definiert.

In jedem Baustein werden die empfohlenen Maßnahmen zum Schluss als Maßnahmenliste aufgeführt. Hierbei war bisher jeder Maßnahme baustein-abhängig eine Priorität zugewiesen, die die Bearbeitungsreihenfolge verdeutlichen sollte. Da sich dies aber durch die Lebenszyklus-Einordnung ergibt, werden an dieser Stelle jetzt die Kategorisierung der Maßnahmen für die Grundschutz-Zertifizierung dargestellt.

Durch die Baustein-Struktur der IT-Grundschutz-Kataloge sollen Redundanzen in den Bausteinen weitgehend vermieden werden. In der Vergangenheit wurden einige Maßnahmen wie [M 3.4 Schulung vor Programmnutzung](#) auf vielen Ebenen angezogen, da hierdurch die unterschiedlichen Sichtweisen bei den verschiedenen Anwendergruppen (z. B. IT-Sicherheitsmanagement und Benutzer) hervorgehoben werden sollte. Da dies aber bei Audits und Basis-Sicherheitschecks zu redundanten Fragen und damit Verzögerungen führt, wurden möglichst viele Redundanzen beseitigt.

# 1 IT-Grundschutz - Basis für IT-Sicherheit

## 1.1 Warum ist IT-Sicherheit wichtig?



Weder ein Unternehmen noch eine Behörde sind mittlerweile ohne funktionierende Informationstechnik (IT) noch lebensfähig. Hierzu gehört auch, dass diese IT sicher betrieben wird. Ein anerkanntes Standardwerk, in dem für die verschiedensten IT-Umgebungen Empfehlungen zum sicheren Umgang mit Information und IT gegeben wird, sind die IT-Grundschutz-Kataloge.

Nahezu alle Geschäftsprozesse und Fachaufgaben werden mittlerweile elektronisch gesteuert. Große Mengen von Informationen werden dabei digital gespeichert, elektronisch verarbeitet und in lokalen und globalen sowie in privaten und öffentlichen Netzen übermittelt. Viele öffentliche oder privatwirtschaftliche Aufgaben und Vorhaben können ohne IT überhaupt nicht mehr oder im besten Fall nur noch teilweise durchgeführt werden. Damit sind viele Institutionen in Verwaltung und Wirtschaft von dem einwandfreien Funktionieren der eingesetzten IT abhängig. Die jeweiligen Behörden- und Unternehmensziele können nur bei ordnungsgemäßem und sicheren IT-Einsatz erreicht werden.

Mit der Abhängigkeit von der IT erhöht sich auch der potenzielle soziale Schaden durch den Ausfall von Informationstechnik. Da IT an sich nicht frei von Schwachstellen ist, besteht ein durchaus berechtigtes Interesse, die von der IT verarbeiteten Daten und Informationen zu schützen und die Sicherheit der IT zu planen, zu realisieren und zu kontrollieren.

Die Schäden durch IT-Fehlfunktionen können verschiedenen Kategorien zugeordnet werden. Am auffälligsten ist der Verlust der Verfügbarkeit: Läuft ein IT-System nicht, können keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind unmöglich, Produktionsprozesse stehen still. Häufig diskutiert ist auch der Verlust der Vertraulichkeit von Daten: Jeder Bürger weiß um die Notwendigkeit, seine personenbezogenen Daten vertraulich zu halten, jedes Unternehmen weiß, dass firmeninterne Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Aber auch der Verlust der Integrität (Korrektheit von Daten) kann schwerwiegende Folgen haben: gefälschte oder verfälschte Daten führen zu Fehlbuchungen, Produktionsprozesse stoppen wegen fehlerhafter Lieferungen, falsche Entwicklungs- und Planungsdaten führen zu fehlerhaften Produkten. Seit einigen Jahren gewinnt auch der Verlust der Authentizität als ein Teilbereich der Integrität an Bedeutung: Daten werden einer falschen Person zugeordnet. Beispielsweise können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die "digitale Identität" wird gefälscht.

Dabei wird diese Abhängigkeit von der Informationstechnik in Zukunft noch weiter zunehmen. Besonders erwähnenswert sind dabei folgende Entwicklungen:

- **Steigender Vernetzungsgrad:** IT-Systeme arbeiten heutzutage nicht mehr isoliert voneinander, sondern werden immer stärker vernetzt. Die Vernetzung ermöglicht es, auf gemeinsame Datenbestände zuzugreifen und intensive Formen der Kooperation über geographische Grenzen hinweg zu nutzen. Damit entsteht nicht nur eine Abhängigkeit von den einzelnen IT-Systemen, sondern in starkem Maße auch von den Datennetzen. Sicherheitsmängel eines IT-Systems können aber dadurch schnell globale Auswirkungen haben.

- **IT-Verbreitung und Durchdringung:** Immer mehr Bereiche werden durch Informationstechnik unterstützt, häufig, ohne dass dies auffällt. Die erforderliche Hardware wird zunehmend kleiner und günstiger, so dass kleine und kleinste IT-Einheiten in alle Bereiche des Alltags integriert werden können. So gibt es beispielsweise Jacken mit integrierten PDAs, RFIDs zur Steuerung von Besucher- oder Warenströmen, IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die Kommunikation der verschiedenen IT-Komponenten untereinander findet dabei zunehmend drahtlos statt.
- **Verschwinden der Netzgrenzen:** Bis vor kurzem ließen sich IT-Anwendungen ganz klar auf die IT-Systeme und die Kommunikationsstrecken dazwischen begrenzen. Ebenso ließ sich sagen, an welchen Standorten und bei welcher Institution diese angesiedelt waren. Durch Globalisierung und die Zunahme von drahtloser und spontaner Kommunikation verschwinden diese Grenzen zunehmend.
- **Angriffe kommen schneller:** Die beste Vorbeugung gegen Computer-Viren, Würmer oder andere Angriffe auf IT-Systeme ist die frühzeitige Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates. Mittlerweile sinkt allerdings die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen darauf, so dass es immer wichtiger wird, ein gut aufgestelltes IT-Sicherheitsmanagement und Warnsystem zu haben.

Angesichts der vorgestellten Gefährdungspotentiale und der steigenden Abhängigkeit stellen sich damit für jede Institution, sei es ein Unternehmen oder eine Behörde, bezüglich IT-Sicherheit mehrere zentrale Fragen:

- Wie sicher ist die Informationstechnik einer Institution?
- Welche IT-Sicherheitsmaßnahmen müssen ergriffen werden?
- Wie müssen diese Maßnahmen konkret umgesetzt werden?
- Wie hält bzw. verbessert eine Institution das erreichte Sicherheitsniveau?
- Wie sicher ist die IT anderer Institutionen, mit denen eine Kooperation stattfindet?

Bei der Suche nach Antworten auf diese Fragen ist zu beachten, dass IT-Sicherheit nicht alleine eine technische Fragestellung ist. Um ein ausreichend sicheres IT-System betreiben zu können, sind neben den technischen auch organisatorische, personelle und baulich-infrastrukturelle Maßnahmen zu realisieren und insbesondere ist ein IT-Sicherheitsmanagement einzuführen, das die Aufgaben zur IT-Sicherheit konzipiert, koordiniert und überwacht.

Vergleicht man jetzt die IT-Systeme aller Institutionen im Hinblick auf obige Fragen, so kristallisiert sich eine besondere Gruppe von IT-Systemen heraus. Die IT-Systeme in dieser Gruppe lassen sich wie folgt charakterisieren:

- Es sind typische IT-Systeme, d. h. diese Systeme sind keine Individuallösungen, sondern sie sind weit verbreitet im Einsatz.
- Der Schutzbedarf der IT-Systeme bezüglich Vertraulichkeit, Integrität und Verfügbarkeit liegt im Rahmen des Normalmaßes.
- Zum sicheren Betrieb der IT-Systeme sind Standard-Sicherheitsmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge erforderlich.

Gelingt es, für diese Gruppe der "typischen" IT-Systeme den gemeinsamen Nenner aller Sicherheitsmaßnahmen, die Standard-Sicherheitsmaßnahmen, zu beschreiben, so würde dies die Beantwortung obiger Fragen für diese "typischen" IT-Systeme erheblich erleichtern. IT-Systeme, die außerhalb

dieser Gruppe liegen, seien es seltenere Individualsysteme oder IT-Systeme mit sehr hohem Schutzbedarf, können sich dann zwar an den Standard-Sicherheitsmaßnahmen orientieren, bedürfen letztlich aber einer individuellen Betrachtung.

Die IT-Grundschutz-Kataloge beschreiben detailliert diese Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Sie umfassen:

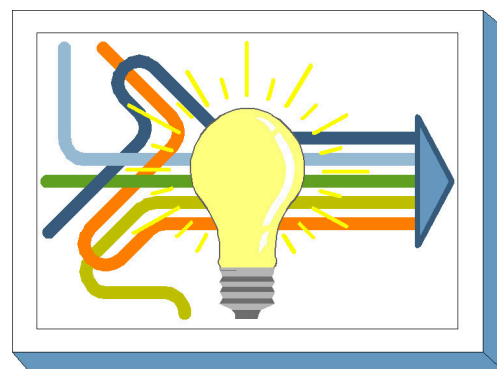
- Standard-Sicherheitsmaßnahmen für typische IT-Systeme mit "normalem" Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage,
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe,
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus und
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs.

Dabei ist die Resonanz sehr positiv. Auf den BSI-Webseiten findet sich ein Auszug aus der Liste derjenigen Institutionen, die IT-Grundschutz einsetzen. Sie stellt im Überblick dar, in welchen Branchen und in welchen Firmen bzw. Behörden IT-Grundschutz angewendet wird.

Da der IT-Grundschutz auch international großen Anklang findet, werden die IT-Grundschutz-Kataloge und das GSTOOL, aber auch die meisten anderen Dokumente zum IT-Grundschutz zusätzlich in englischer Sprache digital zur Verfügung gestellt.

## 1.2 IT-Grundschutz: Ziel, Idee und Konzeption

In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.



Um den sehr heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wider, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren.

Die Vorgehensweise nach IT-Grundschutz hilft dabei, IT-Sicherheitskonzepte einfach und arbeitsökonomisch zu erstellen. Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten IT-Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Bei einer Risikobewertung nach IT-Grundschutz wird hingegen nur ein Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende und noch nicht umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge durch entsprechende individuelle, qualitativ höherwertige Maßnahmen, zu ergänzen. Eine einfache Vorgehensweise hierzu ist in dem BSI-Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschrieben.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die in den IT-Grundschutz-Katalogen nicht hinreichend behandelt werden, bieten diese dennoch eine wertvolle Arbeitshilfe. Die dann notwendige ergänzende Analyse kann sich auf die spezifischen Gefährdungen und Sicherheitsmaßnahmen für diese Komponenten oder Rahmenbedingungen konzentrieren.

Bei den in den IT-Grundschutz-Katalogen aufgeführten Maßnahmen handelt es sich um Standard-Sicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Basis-Sicherheit zu erreichen. Dabei stellen die Maßnahmen, die für die IT-Grundschutz-Zertifizierung gefordert werden, das Minimum dessen dar, was in jedem Fall vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Die als "zusätzlich" gekennzeichneten Maßnahmen haben sich ebenfalls in der Praxis bewährt, sie richten sich jedoch an Anwendungsfälle mit erhöhten Sicherheitsanforderungen.

Sicherheitskonzepte, die auf IT-Grundschutz basieren, können kompakt gehalten werden, da innerhalb des Konzepts jeweils nur auf die entsprechenden Maßnahmen in den IT-Grundschutz-Katalogen ver-



wiesen werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Maßnahmenempfehlungen leichter umsetzbar zu machen, sind die Sicherheitsmaßnahmen in den IT-Grundschutz-Katalogen detailliert beschrieben. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die IT-Grundschutz-Kataloge ebenso wie die meisten Informationen rund um IT-Grundschutz auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt, die teilweise durch das BSI und teilweise auch von IT-Grundschutz-Anwendern bereitgestellt werden.

Da die Informationstechnik sehr innovativ ist und sich ständig weiterentwickelt, sind die vorliegenden Kataloge auf Aktualisierbarkeit und Erweiterbarkeit angelegt. Das Bundesamt für Sicherheit in der Informationstechnik aktualisiert auf der Grundlage von Anwenderbefragungen die IT-Grundschutz-Kataloge ständig und erweitert sie um neue Themen.

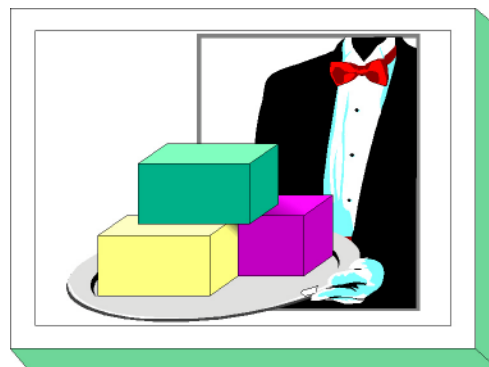
Das BSI bietet allen Anwendern die Möglichkeit der freiwilligen, selbstverständlich kostenfreien Registrierung an. Registrierte Anwender erhalten regelmäßig Informationen über aktuelle Themen des IT-Grundschutzes und der IT-Sicherheit. Die Registrierung ist außerdem die Grundlage für die Anwenderbefragungen. Nur durch den ständigen Erfahrungsaustausch mit den IT-Grundschutz-Anwendern ist eine bedarfsgerechte Weiterentwicklung möglich. Diese Bemühungen zielen letztlich darauf, aktuelle Empfehlungen zu typischen IT-Sicherheitsproblemen aufzeigen zu können. Maßnahmenempfehlungen, die nicht ständig aktualisiert und erweitert werden, veralten sehr schnell oder müssen so generisch gehalten werden, dass sie ihren eigentlichen Nutzen, Sicherheitslücken zu identifizieren und die konkrete Umsetzung zu vereinfachen, verfehlen.

## 1.3 Aufbau der IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge lassen sich in verschiedene Bereiche untergliedern, die zum besseren Verständnis hier kurz erläutert werden sollen:

### Einstieg und Vorgehensweise

In diesem einleitenden Teil wird die Konzeption IT-Grundschutz und die Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach IT-Grundschutz kurz vorgestellt. Eine ausführliche Beschreibung der Vorgehensweise nach IT-Grundschutz findet sich im BSI-Standard 100-2. Außerdem wird die Struktur der IT-Grundschutz-Kataloge und deren Nutzung erläutert.



### IT-Sicherheitsmanagement

Die Planungs- und Lenkungs Aufgabe, die erforderlich ist, um einen durchdachten und planmäßigen IT-Sicherheitsprozess aufzubauen und kontinuierlich umzusetzen, wird als IT-Sicherheitsmanagement bezeichnet.

Die Erfahrung zeigt, dass es ohne ein funktionierendes IT-Sicherheitsmanagement praktisch nicht möglich ist, ein durchgängiges und angemessenes IT-Sicherheitsniveau zu erzielen und zu erhalten. Daher wird im BSI-Standard 100-1 "Managementsysteme für Informationssicherheit (ISMS)" beschrieben, wie ein solches Managementsystem aufgebaut werden kann.

Aufbauend hierauf wird außerdem in Baustein B 1.0 der IT-Grundschutz-Kataloge beschrieben, wie ein effizientes IT-Sicherheitsmanagement aussehen sollte und welche Organisationsstrukturen dafür sinnvoll sind. Es wird außerdem ein systematischer Weg aufgezeigt, wie ein funktionierendes IT-Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann.

### Bausteine

Die Bausteine der IT-Grundschutz-Kataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen und IT-Systeme sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen. Die Bausteine sind nach dem IT-Grundschutz-Schichtenmodell in die folgenden Kataloge gruppiert:

- B 1: Übergeordnete Aspekte der IT-Sicherheit
- B 2: Sicherheit der Infrastruktur
- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

### Gefährdungskataloge

Dieser Bereich enthält die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. Die Gefährdungen sind in fünf Kataloge gruppiert:

- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen



## Maßnahmenkataloge

Dieser Teil beschreibt die in den Bausteinen der IT-Grundsicherheits-Kataloge zitierten IT-Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Maßnahmenkataloge gruppiert:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

## Aufbau der Bausteine

Die zentrale Rolle der IT-Grundsicherheits-Kataloge spielen die Bausteine, deren Aufbau im Prinzip gleich ist. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des IT-Systems.

Im Anschluss daran wird die Gefährdungslage dargestellt. Die Gefährdungen sind dabei nach den genannten Bereichen Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen unterteilt.

Um die Bausteine übersichtlich zu gestalten und um Redundanzen zu vermeiden, werden die Gefährdungstexte lediglich referenziert. Hier ein Beispiel für das Zitat einer Gefährdung innerhalb eines Bausteins:

### - [G 4.1](#) Ausfall der Stromversorgung

Im Kürzel G x.y steht der Buchstabe "G" für Gefährdung. Die Zahl x vor dem Punkt bezeichnet den Gefährdungskatalog (hier G 4 = Technisches Versagen) und die Zahl y nach dem Punkt bezeichnet die laufende Nummer der Gefährdung innerhalb des jeweiligen Katalogs. Es folgt der Titel der Gefährdung. Ein Einlesen in die Gefährdungen ist aus Gründen der Sensibilisierung und des Verständnisses der Maßnahmen empfehlenswert, aber für die Erstellung eines IT-Sicherheitskonzepts nach IT-Grundsicherheits nicht zwingend erforderlich.

Den wesentlichen Teil eines jeden Bausteins bilden die Maßnahmenempfehlungen, die sich an die Gefährdungslage anschließen. Zunächst erfolgen kurze Hinweise zum jeweiligen Maßnahmenbündel. So enthalten diese Ausführungen z. B. Hinweise zur folgerichtigen Reihenfolge bei der Realisierung der notwendigen Maßnahmen.

In jedem Baustein wird für das betrachtete Themengebiet vor der Maßnahmen-Liste eine Übersicht in Form eines "Lebenszyklus" gegeben, welche Maßnahmen in welcher Phase der Bearbeitung zu welchem Zweck umgesetzt werden sollten. In der Regel können die folgenden Phasen identifiziert werden, wobei für jede dieser Phasen typische Arbeiten angegeben sind, die im Rahmen einzelner Maßnahmen durchgeführt werden. Phasenübergreifend wirken dabei das IT-Sicherheitsmanagement und die Revision, die den gesamten Lebenszyklus begleiten und kontrollieren.

Phase	typische Tätigkeiten
Planung und Konzeption	<ul style="list-style-type: none"> <li>- Definition des Einsatzzwecks</li> <li>- Festlegung von Einsatzszenarien</li> <li>- Abwägung des Risikopotentials</li> <li>- Dokumentation der Einsatzentscheidung</li> <li>- Erstellung des IT-Sicherheitskonzepts</li> <li>- Festlegung von Richtlinien für den Einsatz</li> </ul>
Beschaffung (sofern erforderlich)	<ul style="list-style-type: none"> <li>- Festlegung der Anforderungen an zu beschaffende Produkte (nach Möglichkeit auf Basis der Einsatzszenarien der Strategie-Phase)</li> <li>- Auswahl der geeigneten Produkte</li> </ul>
Umsetzung	<ul style="list-style-type: none"> <li>- Konzeption und Durchführung des Testbetriebs</li> <li>- Installation und Konfiguration entsprechend Sicherheitsrichtlinie</li> <li>- Schulung und Sensibilisierung aller Betroffenen</li> </ul>
Betrieb	<ul style="list-style-type: none"> <li>- Sicherheitsmaßnahmen für den laufenden Betrieb (z. B. Protokollierung)</li> <li>- Kontinuierliche Pflege und Weiterentwicklung</li> <li>- Änderungsmanagement</li> <li>- Organisation und Durchführung von Wartungsarbeiten</li> <li>- Audit</li> </ul>
Aussonderung (sofern erforderlich)	<ul style="list-style-type: none"> <li>- Entzug von Berechtigungen</li> <li>- Entfernen von Datenbeständen und Referenzen auf diese Daten</li> <li>- Sichere Entsorgung von Datenträgern</li> </ul>
Notfallvorsorge	<ul style="list-style-type: none"> <li>- Konzeption und Organisation der Datensicherung</li> <li>- Nutzung von Redundanz zur Erhöhung der Verfügbarkeit</li> <li>- Umgang mit Sicherheitsvorfällen</li> <li>- Erstellen eines Notfallplans</li> </ul>

Es finden sich nicht in allen Bausteinen für jede Phase Maßnahmen. So findet sich beispielsweise im Baustein IIS-Server keine Maßnahme in der Beschaffungsphase, da dieser Baustein auf der Umsetzung des Bausteins Webserver basiert und hier die Auswahl eines Produkts bereits entschieden wurde.

Da alle Geschäftsprozesse, IT-Systeme und Einsatzbedingungen sich ständig ändern und weiterentwickelt werden, müssen die Phasen erfahrungsgemäß immer wieder durchlaufen werden. Dies sicherzustellen ist Aufgabe des IT-Sicherheitsmanagements.

Analog zu den Gefährdungen sind die Maßnahmen in die Maßnahmenkataloge Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge gruppiert. Wie bei den Gefährdungen wird hier ebenfalls nur auf die entsprechende Maßnahme referenziert. Hier ein Beispiel für das Zitat einer empfohlenen Maßnahme innerhalb eines Bausteins:

- [M 1.15](#) (A) Geschlossene Fenster und Türen

Im Kürzel M x.y bezeichnet "M" eine Maßnahme, die Zahl x vor dem Punkt den Maßnahmenkatalog (hier M 1 = Infrastruktur). Die Zahl y nach dem Punkt ist die laufende Nummer der Maßnahme innerhalb des jeweiligen Katalogs.

Mit dem Buchstaben in Klammern - hier (A) - wird zu jeder Maßnahme eine Einstufung angegeben, ob sie für die Grundschutz-Qualifizierung gefordert wird. Folgende Einstufungen sind vorgesehen:

A (Einstieg)	Diese Maßnahmen müssen für alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz (Selbsterklärung Einstiegsstufe, Selbsterklärung Aufbaustufe und IT-Grundschutz-Zertifikat) umgesetzt sein. Diese Maßnahmen sind essentiell für die Sicherheit innerhalb des betrachteten Bausteins. Sie sind vorrangig umzusetzen.
B (Aufbau)	Diese Maßnahmen müssen für die Selbsterklärung Aufbaustufe und für das IT-Grundschutz-Zertifikat umgesetzt sein. Sie sind besonders wichtig für den Aufbau einer kontrollierbaren IT-Sicherheit. Eine zügige Realisierung ist anzustreben.
C (Zertifikat)	Diese Maßnahmen müssen für das IT-Grundschutz-Zertifikat umgesetzt sein. Sie sind wichtig für die Abrundung der IT-Sicherheit. Bei Engpässen können sie zeitlich nachrangig umgesetzt werden.
Z (zusätzlich)	Diese Maßnahmen müssen weder für eine Selbsterklärung noch für das IT-Grundschutz-Zertifikat verbindlich umgesetzt werden. Sie stellen Ergänzungen dar, die vor allem bei höheren Sicherheitsanforderungen erforderlich sein können.

Um ein IT-Sicherheitskonzept nach IT-Grundschutz erstellen und den dabei notwendigen Soll-Ist-Vergleich durchführen zu können, ist es erforderlich, die Texte zu den jeweils in den identifizierten Bausteinen enthaltenen Maßnahmen im jeweiligen Maßnahmenkatalog sorgfältig zu lesen. Als Beispiel sei hier ein Auszug aus einer Maßnahme zitiert:

#### **M 2.11      Regelung des Passwortgebrauchs**

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Benutzer

[Maßnahmentext ...]

Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?

[...]

Die Maßnahmentexte sind sinngemäß umzusetzen. Sie sind so geschrieben, dass sie auf möglichst viele Bereiche angewendet werden können. Bevor die Maßnahmenempfehlungen umgesetzt werden, ist immer zu überlegen, ob sie für die jeweilige Organisation oder IT-Umgebungen angepasst werden müssen. Alle Änderungen sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, werden Verantwortliche beispielhaft genannt. *Verantwortlich für die Initiierung* bezeichnet die Personen oder Rollen, die die Umsetzung einer Maßnahme typischerweise veranlassen sollten. *Verantwortlich für die Umsetzung* bezeichnet die Personen oder Rollen, die die Maßnahme realisieren sollten.

Weiterhin werden ergänzende Kontrollfragen angeführt, die das behandelte Thema abrunden und nochmals einen kritischen Blick auf die Umsetzung der Maßnahmen bewirken sollen. Diese ergänzenden Kontrollfragen erheben dabei jedoch keinen Anspruch auf Vollständigkeit.

Der Zusammenhang zwischen den für den IT-Grundschutz angenommenen Gefährdungen und den empfohlenen Maßnahmen kann den Maßnahmen-Gefährdungstabellen entnommen werden. Diese finden sich auf den Grundschutz-Seiten der BSI-Webseite. Für jeden Baustein gibt es eine Maßnahmen-Gefährdungstabelle.

Als Beispiel sei ein Auszug aus der Maßnahmen-Gefährdungstabelle für den Baustein B 2.10 *Mobiler Arbeitsplatz* angeführt:

Priorität/Siegel			G 1. 15	G 2. 1	G 2. 4	G 2. 47	G 2. 48	G 3. 3	G 3. 43	G 3. 44	G 5. 1	G 5. 2	G 5. 4	G 5. 71
<a href="#">M 1.15</a>	1	A									X		X	
<a href="#">M 1.23</a>	1	A									X		X	
<a href="#">M 1.45</a>	1	A				X	X					X	X	X
<a href="#">M 1.46</a>	1	Z											X	
<a href="#">M 1.61</a>	1	A	X					X			X		X	X

Alle Tabellen haben einen einheitlichen Aufbau. In der Kopfzeile sind die im dazugehörigen Baustein aufgelisteten Gefährdungen mit ihren Nummern eingetragen. In der ersten Spalte finden sich entsprechend die Nummern der Maßnahmen wieder. In der zweiten Spalte ist eingetragen, welche Priorität die einzelne Maßnahme für den betrachteten Baustein besitzt. In der dritten Spalte ist notiert, welche Einstufung bezüglich einer Grundschutz-Qualifizierung die einzelne Maßnahme für den betrachteten Baustein besitzt.

Die übrigen Spalten beschreiben den Zusammenhang zwischen Maßnahmen und Gefährdungen. Ist in einem Feld ein "X" eingetragen, so bedeutet dies, dass die korrespondierende Maßnahme gegen die entsprechende Gefährdung wirksam ist. Diese Wirkung kann schadensvorbeugender oder schadensmindernder Natur sein.

Zu beachten ist, dass in den Maßnahmen-Gefährdungstabellen nur die wichtigsten Gefährdungen angeführt sind, gegen die eine bestimmte Maßnahme wirkt. Dies bedeutet insbesondere, dass eine Maßnahme nicht automatisch überflüssig wird, wenn alle in der Tabelle zugeordneten Gefährdungen in einem bestimmten Anwendungsfall nicht relevant sind. Ob auf eine Standard-Sicherheitsmaßnahme verzichtet werden kann, muss immer im Einzelfall anhand der vollständigen Sicherheitskonzeption und nicht nur anhand der Maßnahmen-Gefährdungstabelle geprüft und dokumentiert werden.

Abschließend sei erwähnt, dass sämtliche Bausteine, Gefährdungen, Maßnahmen, Tabellen und Hilfsmittel in elektronischer Form verfügbar sind. Diese Texte können bei der Erstellung eines IT-Sicherheitskonzeptes und bei der Realisierung von Maßnahmen weiterverwendet werden.

## 1.4 Anwendungsweisen der IT-Grundschutz-Kataloge

Für die erfolgreiche Etablierung eines kontinuierlichen und effektiven IT-Sicherheitsprozesses müssen eine ganze Reihe von Aktionen durchgeführt werden. Hierfür bieten die IT-Grundschutz-Vorgehensweise sowie die IT-Grundschutz-Kataloge Hinweise zur Methodik und praktische Umsetzungshilfen. Enthalten sind ferner Lösungsansätze für verschiedene, die IT-Sicherheit betreffende Aufgabenstellungen, beispielsweise IT-Sicherheitskonzeption, Revision und Qualifizierung. Je nach vorliegender Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig. Dieser Abschnitt dient dazu, durch Querverweise auf die entsprechenden Kapitel der IT-Grundschutz-Vorgehensweise den direkten Einstieg in die einzelnen Anwendungsweisen zu erleichtern.



### IT-Sicherheitsprozess und IT-Sicherheitsmanagement

Die Abhängigkeit vom ordnungsgemäßen Funktionieren der Informationstechnik hat in den letzten Jahren sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft stark zugenommen. Immer mehr Geschäftsprozesse werden auf die Informationstechnik verlagert oder mit ihr verzahnt. Ein Ende dieser Entwicklung ist nicht abzusehen. IT-Sicherheit ist daher als integraler Bestandteil der originären Aufgabe anzusehen. Der folgende Aktionsplan beinhaltet alle wesentlichen Schritte, die für einen kontinuierlichen IT-Sicherheitsprozess notwendig sind, und ist somit als eine planmäßig anzuwendende, begründete Vorgehensweise zu verstehen, wie ein angemessenes IT-Sicherheitsniveau erreicht und aufrechterhalten werden kann:

- Initiierung des IT-Sicherheitsprozesses:
  - Übernahme von Verantwortung durch die Leitungsebene
  - Konzeption und Planung des IT-Sicherheitsprozesses
  - Aufbau einer IT-Sicherheitsorganisation
  - Bereitstellung von Ressourcen für die IT-Sicherheit
- Erstellung einer IT-Sicherheitskonzeption
- Umsetzung der IT-Sicherheitskonzeption
  - Realisierung der IT-Sicherheitsmaßnahmen
  - Einbindung aller Mitarbeiter in den IT-Sicherheitsprozess
- Aufrechterhaltung der IT-Sicherheit und kontinuierliche Verbesserung

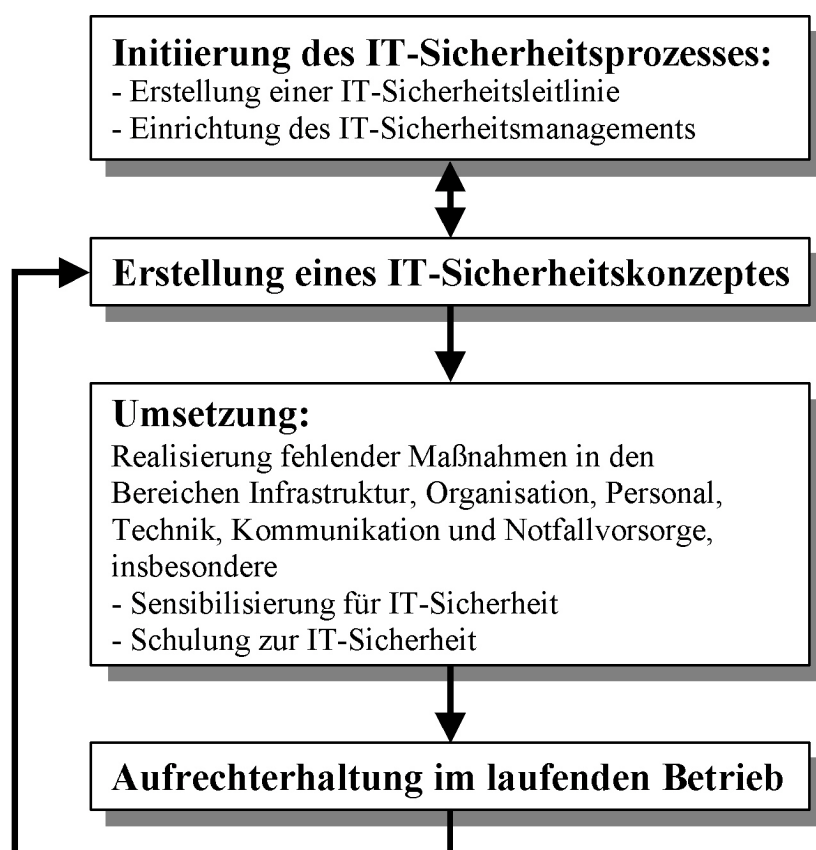


Abbildung: Initiierung des IT-Sicherheitsprozesses

Im Dokument IT-Grundschutz-Vorgehensweise wird dies ausführlich beschrieben. Außerdem wird im Baustein B 1.0 *IT-Sicherheitsmanagement* der IT-Sicherheitsprozess im Überblick dargestellt und es wird eine detaillierte Erläuterung der einzelnen Aktionen in Form empfohlener Standard-Maßnahmen gegeben.

Zur Erstellung der IT-Sicherheitskonzeption ist nach IT-Grundschutz eine Reihe von Schritten notwendig. Eine kurze Darstellung davon wird im Folgenden gegeben.

### IT-Strukturanalyse

Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Für die Erstellung eines IT-Sicherheitskonzepts und insbesondere für die Anwendung von IT-Grundschutz ist es erforderlich, die Struktur der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen bietet sich ein Netztopologieplan als Ausgangsbasis für die Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

- die vorhandene Infrastruktur,
- die organisatorischen und personellen Rahmenbedingungen für den IT-Verbund,
- im IT-Verbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,

- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen,
- im IT-Verbund betriebene IT-Anwendungen.

Die einzelnen Schritte der IT-Strukturanalyse werden im Detail in Kapitel 4.1 der IT-Grundschutz-Vorgehensweise in Form einer Handlungsanweisung beschrieben.

### **Schutzbedarfsfeststellung**

Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Erläuterungen und praktische Hinweise zur Schutzbedarfsfeststellung sind Gegenstand von Kapitel 4.2 der IT-Grundschutz-Vorgehensweise.

### **Modellierung**

Im nächsten Schritt müssen die Bausteine der IT-Grundschutz-Kataloge in einem Modellierungsschritt auf die Komponenten des vorliegenden IT-Verbunds abgebildet werden.

In Kapitel 4.3 der IT-Grundschutz-Vorgehensweise wird beschrieben, wie die Modellierung eines IT-Verbunds durch Bausteine aus den IT-Grundschutz-Katalogen vorgenommen werden sollte. Detaillierte Hinweise für die Verwendung des Schichtenmodells und die Modellierung nach IT-Grundschutz sind im Kapitel "Modellierung" enthalten. Wie der anschließende Soll-Ist-Vergleich anhand eines Basis-Sicherheitschecks durchgeführt werden sollte, wird in Kapitel 4.4 der IT-Grundschutz-Vorgehensweise beschrieben.

### **Basis-Sicherheitscheck**

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene IT-Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status Quo eines bestehenden (nach IT-Grundschutz modellierten) IT-Verbunds in Bezug auf den Umsetzungsgrad von Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge ermittelt. Als Ergebnis liegt eine Übersicht vor, in dem für jede relevante Maßnahme der Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise umgesetzten Maßnahmen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Informationstechnik aufgezeigt. Kapitel 4.4 beschreibt einen Aktionsplan für die Durchführung eines Basis-Sicherheitschecks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

### **IT-Sicherheitsrevision**

Die in den IT-Grundschutz-Katalogen enthaltenen Sicherheitsmaßnahmen können auch für die IT-Sicherheitsrevision genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim Basis-Sicherheitscheck empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein anhand der Maßnahmentexte eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und verbessert häufig die Reproduzierbarkeit der Ergebnisse.

### **Weiterführende IT-Sicherheitsmaßnahmen**

Die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Bei hohem oder sehr hohem Schutzbedarf kann es jedoch sinnvoll sein zu prüfen, ob zusätzlich oder ersatzweise höherwertige IT-Sicherheitsmaßnahmen erforderlich sind. Geeignete Maßnahmen für Bereiche mit höherem Schutzbedarf sollten über ergänzende Sicherheitsanalysen ausgewählt werden.



Eine Methode hierfür ist die im BSI-Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschriebene Vorgehensweise.

### **Umsetzung von IT-Sicherheitskonzepten**

Damit das angestrebte IT-Sicherheitsniveau erreicht wird, müssen bestehende Schwachstellen ermittelt und alle erforderlichen Maßnahmen identifiziert werden. Diese sowie die Realisierungsplanung müssen in einem Sicherheitskonzept festgehalten werden. Vor allem müssen alle erforderlichen Maßnahmen auch konsequent umgesetzt werden. In Kapitel 4.6 des Dokuments zur IT-Grundschutz-Vorgehensweise wird beschrieben, was bei der Umsetzungsplanung von IT-Sicherheitsmaßnahmen beachtet werden muss.

### **Zertifizierung nach IT-Grundschutz**

Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge werden nicht nur für die IT-Sicherheitskonzeption, sondern auch zunehmend als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine IT-Grundschutz-Zertifizierung kann eine Institution nach innen und außen hin dokumentieren, dass sie IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat.

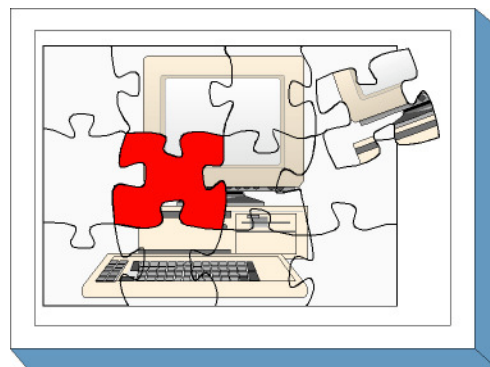
Das Niveau der Qualifizierung wird dabei in drei verschiedene Stufen unterteilt, die sich sowohl im Hinblick auf die Güte (d. h. den erforderlichen Umsetzungsgrad der Sicherheitsmaßnahmen) als auch in Bezug auf die Vertrauenswürdigkeit unterscheiden. Das Eingangsniveau kann durch einen Mitarbeiter der Institution selbst nachgewiesen werden, das höchste Niveau erfordert eine Prüfung durch unabhängige Dritte. Das Prüfungsschema für IT-Grundschutz-Zertifizierungen sowie das Lizenzierungsschema für Auditoren ist im Dokument "ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz" beschrieben.



## 2 Schichtenmodell und Modellierung

### 2.1 Modellierung nach IT-Grundschatz

Bei der Umsetzung von IT-Grundschatz muss der betrachtete IT-Verbund mit Hilfe der vorhandenen Bausteine nachgebildet werden, also die relevanten Sicherheitsmaßnahmen aus den IT-Grundschatz-Katalogen zusammengetragen werden. Dafür müssen die IT-Strukturanalyse und eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschatzmodell des IT-Verbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschatz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des IT-Verbunds beinhaltet.



Das erstellte IT-Grundschatzmodell ist unabhängig davon, ob der IT-Verbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen IT-Verbund handelt, der sich erst im Planungsstadium befindet. Jedoch kann das Modell unterschiedlich verwendet werden:

- Das IT-Grundschatzmodell eines bereits realisierten IT-Verbunds identifiziert über die verwendeten Bausteine die relevanten Standard-Sicherheitsmaßnahmen. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschatzmodell eines geplanten IT-Verbunds stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Standard-Sicherheitsmaßnahmen bei der Realisierung des IT-Verbunds umgesetzt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht das folgende Bild:

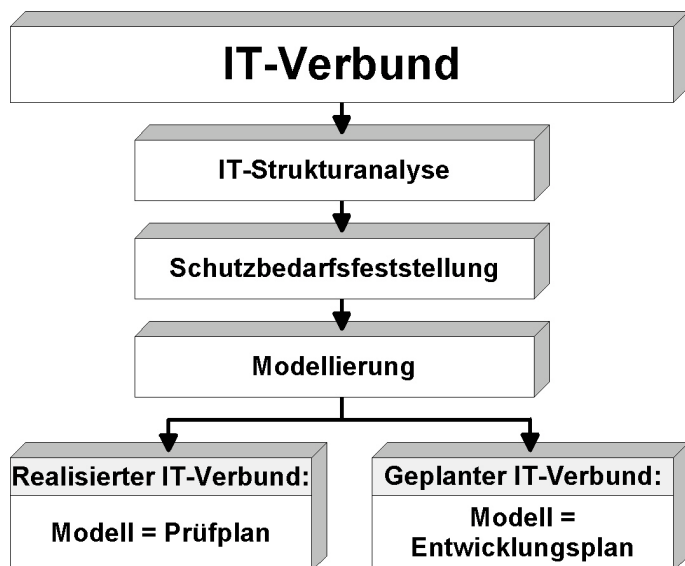


Abbildung: Ergebnis der Modellierung nach IT-Grundschatz

Typischerweise wird ein im Einsatz befindlicher IT-Verbund sowohl realisierte als auch in Planung befindliche Anteile besitzen. Das resultierende IT-Grundschatzmodell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts.

Für die Abbildung eines im Allgemeinen komplexen IT-Verbunds auf die Bausteine der IT-Grundschutz-Kataloge bietet es sich an, die IT-Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

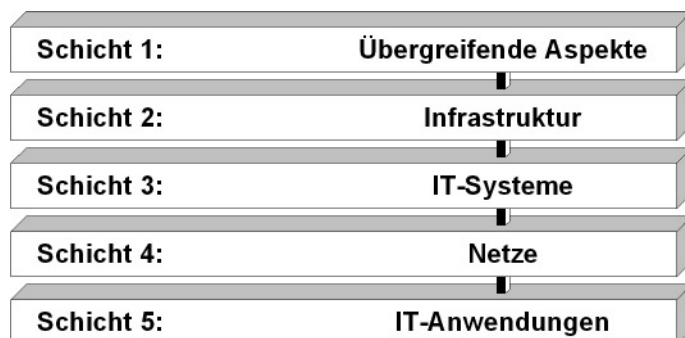


Abbildung: Schichten des IT-Grundschutzmodells

Die IT-Sicherheitsaspekte eines IT-Verbunds werden wie folgt den einzelnen Schichten zugeordnet:

- **Schicht 1** umfasst die übergreifenden IT-Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.
- **Schicht 2** befasst sich mit den baulich-physischen Gegebenheiten. In dieser Schicht werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft zum Beispiel die Bausteine Gebäude, Serverraum, Schutzschrank und häuslicher Arbeitsplatz.
- **Schicht 3** betrifft die einzelnen IT-Systeme des IT-Verbunds, die gegebenenfalls in Gruppen zusammengefasst wurden. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. In diese Schicht fallen beispielsweise die Bausteine TK-Anlage, Laptop sowie Client unter Windows 2000.
- **Schicht 4** betrachtet die Vernetzungsaspekte, die sich in erster Linie nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Heterogene Netze, Modem sowie Remote Access.
- **Schicht 5** schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund genutzt werden. In dieser Schicht können unter anderem die Bausteine E-Mail, Webserver, Faxserver und Datenbanken zur Modellierung verwendet werden.

Die Aufgabenstellung bei der Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des IT-Verbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten, usw.

Nachfolgend wird die Vorgehensweise der Modellierung für einen IT-Verbund detailliert beschrieben. Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

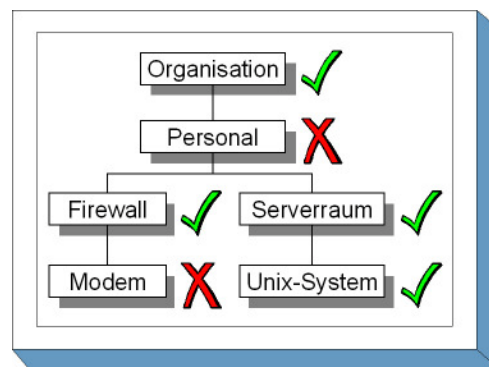
Bei der Modellierung eines IT-Verbunds nach IT-Grundschutz kann das Problem auftreten, dass es Zielobjekte gibt, die mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden können. In diesem Fall sollte eine ergänzenden Sicherheitsanalyse durchgeführt werden, wie in der IT-Grundschutz-Vorgehensweise beschrieben.

## 2.2 Zuordnung anhand Schichtenmodell

Bei der Modellierung eines IT-Verbunds ist es zweckmäßig, die Zuordnung der Bausteine anhand des Schichtenmodells vorzunehmen. Daran anschließend folgt schließlich die Vollständigkeitsprüfung.

### zu Schicht 1: Übergeordnete Aspekte der IT-Sicherheit

In dieser Schicht werden alle Aspekte des IT-Verbunds modelliert, die den technischen Komponenten übergeordnet sind. Im Vordergrund stehen dabei Konzepte und die von diesen Konzepten abgeleiteten Regelungen. Diese Aspekte sollten für den gesamten IT-Verbund einheitlich geregelt sein, so dass die entsprechenden Bausteine in den meisten Fällen nur einmal für den gesamten IT-Verbund anzuwenden sind. Dem IT-Sicherheitsmanagement, der Organisation des IT-Betriebs sowie der Schulung und Sensibilisierung des Personals kommt dabei eine besondere Bedeutung zu. Die Umsetzung der diesbezüglichen Maßnahmen ist von grundlegender Bedeutung für die sichere Nutzung von Informations- und Kommunikationstechnik. Unabhängig von den eingesetzten technischen Komponenten sind die entsprechenden Bausteine daher immer anzuwenden.



- Der Baustein B 1.0 *IT-Sicherheitsmanagement* ist für den gesamten IT-Verbund einmal anzuwenden. Ein funktionierendes IT-Sicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.1 *Organisation* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.2 *Personal* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.3 *Notfallvorsorge-Konzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Verfügbarkeit haben oder wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei der Bearbeitung des Bausteins ist besonderes Augenmerk auf diese Komponenten zu richten. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.4 *Datensicherungskonzept* ist für den gesamten IT-Verbund einmal anzuwenden.
- Der Baustein B 1.6 *Computer-Virenschutzkonzept* ist für den gesamten IT-Verbund einmal anzuwenden.

- Der Baustein B 1.7 *Kryptokonzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit oder Integrität haben, oder wenn bereits kryptographische Verfahren im Einsatz sind.
- Der Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf einen der drei Grundwerte haben, oder wenn der Ausfall des gesamten IT-Verbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.9 *Hard- und Software-Management* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.10 *Standardsoftware* ist zumindest einmal für den gesamten IT-Verbund anzuwenden. Gibt es innerhalb des IT-Verbunds Teilbereiche mit unterschiedlichen Anforderungen oder Regelungen für die Nutzung von Standardsoftware, sollte Baustein B 1.10 auf diese Teilbereiche jeweils getrennt angewandt werden.
- Der Baustein B 1.11 *Outsourcing* ist zumindest dann anzuwenden, wenn die folgenden Bedingungen alle erfüllt sind:
  - IT-Systeme, Anwendungen oder Geschäftsprozesse werden zu einem externen Dienstleister ausgelagert, und
  - die Bindung an den Dienstleister erfolgt auf längere Zeit, und
  - durch die Dienstleistung kann die IT-Sicherheit des Auftraggebers beeinflusst werden, und
  - im Rahmen der Dienstleistungen erbringt der Dienstleister auch regelmäßig nennenswerte IT-Sicherheitsmanagement-Tätigkeiten.

Gibt es in einem IT-Verbund verschiedene ausgelagerte Komponenten bei unterschiedlichen Dienstleistern, ist der Baustein für jeden externen Dienstleister einmal anzuwenden. Für die Anwendung dieses Bausteins gelten besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

- Der Baustein B 1.12 *Archivierung* ist auf den IT-Verbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.
- Der Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung* ist für den gesamten IT-Verbund einmal anzuwenden.

## zu Schicht 2: Sicherheit der Infrastruktur

Die für den vorliegenden IT-Verbund relevanten baulichen Gegebenheiten werden mit Hilfe der Bausteine aus Schicht 2 "Sicherheit der Infrastruktur" modelliert. Jedem Gebäude, Raum oder Schutzschrank (bzw. Gruppen dieser Komponenten) wird dabei der entsprechende Baustein aus den IT-Grundschutz-Katalogen zugeordnet.

- Der Baustein B 2.1 *Gebäude* ist für jedes Gebäude bzw. jede Gebäudegruppe einmal anzuwenden.

- Der Baustein B 2.2 *Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1). Falls bestimmte Teilbereiche - beispielsweise Serverraum oder Leitstand - in Bezug auf die Verkabelung Besonderheiten aufweisen, kann es jedoch zweckmäßig sein, Baustein B 2.2 an diesen Stellen gesondert anzuwenden.
- Der Baustein B 2.3 *Bürraum* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Informationstechnik genutzt wird, für die jedoch keiner der Bausteine B 2.4, B 2.5, B 2.6, B 2.8, B 2.9, B 2.10 oder B 2.11 herangezogen wird.
- Der Baustein B 2.4 *Serverraum* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Server oder TK-Anlagen betrieben werden. Server sind IT-Systeme, die Dienste im Netz zur Verfügung stellen. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.
- Der Baustein B 2.5 *Datenträgerarchiv* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Datenträger gelagert oder archiviert werden.
- Der Baustein B 2.6 *Raum für technische Infrastruktur* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen technische Geräte betrieben werden, die keine oder nur wenig Bedienung erfordern (z. B. Verteilerschrank, Netzersatzanlage).
- Der Baustein B 2.7 *Schutzschränke* ist auf jeden Schutzschrank bzw. jede Gruppe von Schutzschränken einmal anzuwenden. Schutzschränke können gegebenenfalls als Ersatz für einen dedizierten Serverraum dienen.
- Der Baustein B 2.8 *Häuslicher Arbeitsplatz* ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.
- Der Baustein B 2.9 *Rechenzentrum* ist auf jedes Rechenzentrum einmal anzuwenden. Als Rechenzentrum werden Einrichtungen und Räumlichkeiten bezeichnet, die für den Betrieb einer größeren, zentral für mehrere Stellen eingesetzten Datenverarbeitungsanlage erforderlich sind. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.
- Der Baustein B 2.10 *Mobiler Arbeitsplatz* ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten des Unternehmens bzw. der Behörde arbeiten, sondern an wechselnden Arbeitsplätzen außerhalb. Typische Zielobjekte für den Baustein B 2.10 sind Laptops.
- Der Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist auf jeden solchen Raum bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.

### zu Schicht 3: Sicherheit der IT-Systeme

Sicherheitsaspekte, die sich auf IT-Systeme beziehen, werden in dieser Schicht abgedeckt. Diese Schicht ist zur Übersichtlichkeit nach Servern, Clients, Netzkomponenten und Sonstiges sortiert.

Analog zum Bereich "Sicherheit der Infrastruktur" können die Bausteine des Bereichs "Sicherheit der IT-Systeme" sowohl auf einzelne IT-Systeme als auch auf Gruppen solcher IT-Systeme angewandt werden. Dies wird im Folgenden nicht mehr gesondert hervorgehoben.

#### Server

- Der Baustein B 3.101 *Allgemeiner Server* ist auf jedes IT-System anzuwenden, das Dienste (z. B. Datei- oder Druckdienste) als Server im Netz anbietet.
- Der Baustein B 3.102 *Server unter Unix* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

- Der Baustein B 3.103 *Server unter Windows NT* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.104 *Server unter Novell Netware 3.x* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.105 *Server unter Novell Netware Version 4.x* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.106 *Server unter Windows 2000* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.107 *S/390- und zSeries-Mainframe* ist auf jeden Großrechner anzuwenden, der vom Typ S/390 oder zSeries ist.

Hinweis: Für jeden Server (und auch jeden Großrechner) muss neben dem Betriebssystem-spezifischen Baustein immer auch Baustein B 3.101 angewandt werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Server zusammengefasst sind.

### Clients

- Der Baustein B 3.201 *Allgemeiner Client* ist auf jeden Client anzuwenden.
- Der Baustein B 3.202 *Allgemeines nicht vernetztes IT-System* ist auf jedes Einzelplatz-System anzuwenden.
- Der Baustein B 3.203 *Laptop* ist auf jeden mobilen Computer (Laptop) anzuwenden.
- Der Baustein B 3.204 *Client unter Unix* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.205 *Client unter Windows NT* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.206 *Client unter Windows 95* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.207 *Client unter Windows 2000* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.208 *Internet-PC* ist auf jeden Computer anzuwenden, der *ausschließlich* für die Nutzung von Internet-Diensten vorgesehen ist und *nicht* mit dem internen Netz der Institution verbunden ist. In diesem speziellen Szenario brauchen *keine weiteren Bausteine* der IT-Grundschatz-Kataloge auf diesen Computer (bzw. diese Gruppe) angewandt werden.
- Der Baustein B 3.209 *Client unter Windows XP* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Client muss neben dem Betriebssystem-spezifischen Baustein immer auch entweder Baustein B 3.201 oder Baustein B 3.202 angewandt werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.

### Netzkomponenten

- Der Baustein B 3.301 *Sicherheitsgateway (Firewall)* ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung (z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern). Aber auch bei einer Kopplung von zwei organisationsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B.



bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.

- Der Baustein B 3.302 *Router und Switches* ist in jedem aktiven Netz, das im vorliegenden IT-Verbund eingesetzt wird, anzuwenden.

#### Sonstiges

- Der Baustein B 3.401 *TK-Anlage* ist auf jede **TK-Anlage** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.402 *Faxgerät* ist auf jedes **Faxgerät** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.403 *Anrufbeantworter* ist auf jeden **Anrufbeantworter** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.404 *Mobiltelefon* sollte mindestens einmal angewandt werden, wenn die Benutzung von Mobiltelefonen in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist.

Bestehen mehrere unterschiedliche Einsatzbereiche von Mobiltelefonen (beispielsweise mehrere Mobiltelefon-Pools), so ist der Baustein B 3.404 jeweils getrennt darauf anzuwenden.

- Der Baustein B 3.405 *PDA* sollte mindestens einmal angewandt werden, wenn die Benutzung von PDAs in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist.

#### zu Schicht 4: Sicherheit im Netz

In dieser Schicht werden Sicherheitsaspekte im Netz behandelt, die nicht an bestimmten IT-Systemen (z. B. Servern) festgemacht werden können. Vielmehr geht es um Sicherheitsaspekte, die sich auf die Netzverbindungen und die Kommunikation zwischen den IT-Systemen beziehen.

Um die Komplexität zu verringern, ist es sinnvoll, bei der Untersuchung statt des Gesamtnetzes Teilbereiche jeweils einzeln zu betrachten. Die hierzu erforderliche Aufteilung des Gesamtnetzes in Teilnetze sollte anhand der beiden folgenden Kriterien vorgenommen werden:

- Im Rahmen der Schutzbedarfsfeststellung sind Verbindungen identifiziert worden, über die bestimmte Daten auf keinen Fall transportiert werden dürfen. Diese Verbindungen bieten sich als "Schnittstellen" zwischen Teilnetzen an, d. h. die Endpunkte einer solchen Verbindung sollten in verschiedenen Teilnetzen liegen. Umgekehrt sollten Verbindungen, die Daten mit hohem oder sehr hohem Schutzbedarf transportieren, möglichst keine Teilnetzgrenzen überschreiten. Dies führt zu einer Definition von Teilnetzen mit möglichst einheitlichem Schutzbedarf.
- Komponenten, die nur über eine Weitverkehrsverbindung miteinander verbunden sind, sollten nicht demselben Teilnetz zugeordnet werden, d. h. Teilnetze sollten sich nicht über mehrere Standorte oder Liegenschaften erstrecken. Dies ist sowohl aus Gründen der Übersichtlichkeit als auch im Hinblick auf eine effiziente Projektdurchführung wünschenswert.

Falls diese beiden Kriterien nicht zu einer geeigneten Aufteilung des Gesamtnetzes führen (beispielsweise weil einige resultierende Teilnetze zu groß oder zu klein sind), kann die Aufteilung in Teilnetze alternativ auch auf organisatorischer Ebene erfolgen. Dabei werden die Zuständigkeitsbereiche der einzelnen Administratoren(-Teams) als Teilnetze betrachtet.

Es ist nicht möglich, eine grundsätzliche Empfehlung darüber zu geben, welche Aufteilung in Teilnetze zu bevorzugen ist, falls die oben angegebenen Anforderungen mit dem vorliegenden IT-Verbund grundsätzlich nicht vereinbar sind. Stattdessen sollte im Einzelfall entschieden werden, welche Auftei

lung des Gesamtnetzes im Hinblick auf die anzuwendenden Bausteine der IT-Grundschatz-Kataloge am praktikabelsten ist.

- Der Baustein B 4.1 *Heterogene Netze* ist in der Regel auf jedes Teilnetz einmal anzuwenden. Falls die Teilnetze klein sind und mehrere Teilnetze in der Zuständigkeit des gleichen Administratoren-Teams liegen, kann es jedoch ausreichend sein, den Baustein B 4.1 auf diese Teilnetze insgesamt einmal anzuwenden.
- Der Baustein B 4.2 *Netz- und Systemmanagement* ist auf jedes Netz- bzw. Systemmanagement-System anzuwenden, das im vorliegenden IT-Verbund eingesetzt wird.
- Der Baustein B 4.3 *Modem* ist auf alle Außenverbindungen anzuwenden, die über Modems realisiert sind.
- Der Baustein B 4.4 *Remote Access* ist pro entfernter Zugriffsmöglichkeit auf das interne Netz, die nicht über eine dedizierte Standleitung erfolgt, einmal anzuwenden (z. B. Telearbeit, Anbindung von Außendienstmitarbeitern über analoge Wählleitungen, ISDN oder Mobiltelefon).
- Der Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* ist auf alle Außenverbindungen anzuwenden, die über ISDN realisiert sind.

#### zu Schicht 5: Sicherheit in Anwendungen

In der untersten Schicht des zu modellierenden IT-Verbunds erfolgt die Nachbildung der Anwendungen. Moderne Anwendungen beschränken sich nur selten auf ein einzelnes IT-System. Insbesondere behörden- bzw. unternehmensweite Kernanwendungen sind in der Regel als Client-Server-Applikationen realisiert. In vielen Fällen greifen Server selbst wieder auf andere, nachgeschaltete Server, z. B. Datenbank-Systeme, zu. Die Sicherheit der Anwendungen muss daher unabhängig von den IT-Systemen und Netzen betrachtet werden.

- Der Baustein B 5.1 *Peer-to-Peer-Dienste* ist auf jeden Client anzuwenden, der Peer-to-Peer-Dienste (beispielsweise freigegebene Verzeichnisse) im Netz anbietet.
- Der Baustein B 5.2 *Datenträgeraustausch* sollte für jede Anwendung einmal herangezogen werden, die als Datenquelle für einen Datenträgeraustausch dient oder auf diesem Wege eingegangene Daten weiterverarbeitet.
- Der Baustein B 5.3 *E-Mail* ist auf jedes E-Mail-System (intern oder extern) des betrachteten IT-Verbunds anzuwenden.
- Der Baustein B 5.4 *Webserver* ist auf jeden WWW-Dienst (z. B. Intranet oder Internet) des betrachteten IT-Verbunds anzuwenden.
- Der Baustein B 5.5 *Lotus Notes* ist auf jedes Workgroup-System, das auf dem Produkt Lotus Notes basiert, bzw. auf jede entsprechende Gruppe im IT-Verbund einmal anzuwenden.
- Der Baustein B 5.6 *Faxserver* ist auf jeden Faxserver bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 5.7 *Datenbanken* sollte pro Datenbanksystem bzw. pro Gruppe von Datenbanksystemen einmal angewandt werden.
- Der Baustein B 5.8 *Telearbeit* ist zusätzlich auf jedes IT-System anzuwenden, das für Telearbeit verwendet wird.
- Der Baustein B 5.9 *Novell eDirectory* sollte auf jeden Verzeichnisdienst, der mit Hilfe von Novell eDirectory realisiert ist, einmal angewandt werden.



- Der Baustein B 5.10 *Internet Information Server* ist - zusätzlich zu Baustein B 5.4 - auf jeden WWW-Dienst anzuwenden, der mit diesem Produkt betrieben wird.
- Der Baustein B 5.11 *Apache Webserver* ist - zusätzlich zu Baustein B 5.4 - auf jeden WWW-Dienst anzuwenden, der mit diesem Produkt betrieben wird.
- Der Baustein B 5.12 *Exchange 2000 / Outlook 2000* ist - zusätzlich zu Baustein B 5.3 - auf jedes Workgroup- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert.

### **Prüfung auf Vollständigkeit**

Abschließend muss überprüft werden, ob die Modellierung des Gesamtsystems vollständig ist und keine Lücken aufweist. Es wird empfohlen, hierzu erneut den Netzplan oder eine vergleichbare Übersicht über den IT-Verbund heranzuziehen und die einzelnen Komponenten systematisch durchzugehen. Jede Komponente muss entweder einer Gruppe zugeordnet oder einzeln modelliert worden sein.

Falls das Gesamtnetz in der Schicht 4 in Teilnetze aufgeteilt wurde, muss geprüft werden, ob

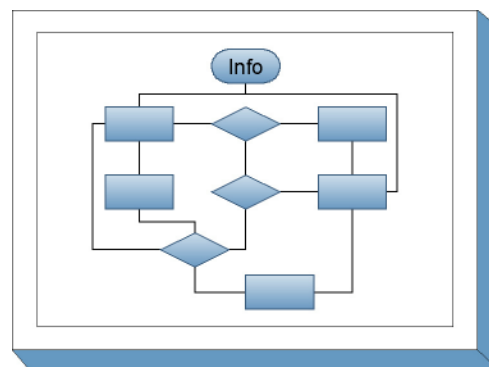
- jedes Teilnetz vollständig nachgebildet wurde und
- durch die Summe aller Teilnetze das Gesamtnetz vollständig dargestellt wird.

Wichtig ist, dass nicht nur alle Hard- und Software-Komponenten in technischer Hinsicht nachgebildet sind, sondern dass auch die zugehörigen organisatorischen, personellen und infrastrukturellen Aspekte vollständig abgedeckt sind.

Falls sich bei der Überprüfung Lücken in der Modellierung zeigen, sind die entsprechenden fehlenden Bausteine hinzuzufügen. Andernfalls besteht die Gefahr, dass wichtige Bestandteile des Gesamtsystems oder wichtige Sicherheitsaspekte bei der Anwendung des IT-Grundschatzes nicht berücksichtigt werden.

### 3 Rollen

In den Maßnahmen der IT-Grundschatz-Kataloge werden neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, Verantwortliche für die Initiierung bzw. für die Umsetzung dieser Maßnahmen beispielhaft genannt. Da die Bezeichnungen der hier als Verantwortlichen genannten Personen oder Rollen nicht in allen Organisationen einheitlich ist, wird für eine leichtere Zuordnung hier eine kurze Rollenbeschreibung dargestellt.



Verantwortliche	Rollenbeschreibung
Administrator	Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems.
Anwendungsentwickler	Ein Anwendungsentwickler ist ein mit der Planung, Entwicklung, Test oder Pflege von Programmen betrauter Experte.
Archivverwalter	Der Archivverwalter ist verantwortlich für Einrichtung, Betrieb, Überwachung und Wartung eines Archivsystems auf fachlicher Ebene.
Bauausführende Firma	Dies sind Firmen, die Bauleistungen aller Art im Auftrag der IT-betreibenden Organisation oder der dazu Beauftragten ausführen. Dies können klassische Baugewerke, Elektrogewerke aber auch die Errichtung von Einrichtungen der Gefahrenmeldetechnik (Errichterfirma) sein.
Bauleiter	Ein Bauleiter ist für die Umsetzung von Baumaßnahmen verantwortlich.
Bauplaner	Die Funktion des Bauplaners (von der Gesamtplanung über Standortplanung etc. bis hin zu Einzelgewerken) kann beispielsweise von einem Architekten oder von einem Planungsbüro wahrgenommen werden.
Behörden-/Unternehmensleitung	Dies bezeichnet die Leitungsebene der Institution bzw. der betrachteten Organisationseinheit.
Beschaffer	Dies bezeichnet einen Mitarbeiter der Beschaffungsstelle, der verantwortlich ist für die Beschaffung von Betriebsmitteln oder IT-Systemen.
Beschaffungsstelle	Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab.
Brandschutzbeauftragter	Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.

Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die für den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde verantwortlich ist.
Fachabteilung	Eine Fachabteilung ist ein Teil einer Behörde bzw. eines Unternehmens, die meist eine oder mehrere Fachaufgaben zu erledigen hat. Bei Bundes- und Landesbehörden stellt die Abteilung den Zusammenschluss mehrerer Referate dar.
Fachverantwortliche	Der Fachverantwortliche ist inhaltlich für ein oder mehrere IT-Verfahren verantwortlich (so ist z. B. bei der Anwendung "automatisierter Vertrieb" der Fachverantwortliche der Referatsleiter Vertrieb).
Fax-Absender	Hiermit ist die Person gemeint, die ein Fax versendet.
Fax-Verantwortlicher	Der Fax-Verantwortliche ist für alle organisatorischen und technischen Regelungen verantwortlich, die die Fax-Nutzung innerhalb einer Organisationseinheit betreffen.
Haustechnik	Haustechnik bezeichnet die Organisationseinheit, die für die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft verantwortlich ist. Betreute Gewerke können dabei z. B. sein: Elektrotechnik, Melde- und Steuerungstechnik, Sicherungstechnik, IT-Netze (Physikalischer Teil), Heizungs- und Sanitärtechnik, Aufzüge etc.
Innerer Dienst	Der Innere Dienst ist eine Organisationseinheit, die alle zentralen Dienste für alle Mitarbeiter koordiniert, z. B. Poststelle, Kopierer, Fahrdienst, Botendienst, Beseitigung technischer Störungen, Gebäudereinigung, Bereitstellung von Betriebsmitteln etc.
IT-Benutzer	Ein IT-Benutzer ist ein Mitarbeiter des Unternehmens bzw. der Behörde, der informationstechnische Systeme für die Erledigung seiner Aufgaben benutzt.
IT-Betreuer	Zu den Aufgaben von IT-Betreuer zählen u. a. die Entgegennahme und Bearbeitung von Benutzeranfragen zu Problemen mit der Standard-IT-Ausstattung.
IT-Sicherheitsbeauftragter	Ein IT-Sicherheitsbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung ernannte Person, die im Auftrag der Leitungsebene für die Ausgestaltung bzw. Umsetzung ausreichender IT-Sicherheit im Unternehmen bzw. in der Behörde verantwortlich ist.
IT-Sicherheitsmanagement	Das IT-Sicherheitsmanagement ist diejenige Personengruppe, die für den IT-Sicherheitsprozess innerhalb einer Organisation verantwortlich ist. Der Begriff IT-Sicherheitsmanagement wird synonym als Bezeichnung für das IT-Sicherheitsmanagement-Team verwendet.
IT-Sicherheitsmanagement-Team	Das IT-Sicherheitsmanagement-Team regelt abteilungsübergreifende Belange zum Thema IT-Sicherheit und erarbeitet Pläne, Vorgaben und Richtlinien zu diesem Thema.

IT-Verfahrensverantwortlicher	Ein IT-Verfahrensverantwortlicher ist für den korrekten Ablauf eines oder mehrere spezieller IT-Verfahren verantwortlich, z. B. für die elektronische Lagerhaltung, etc.
Leiter Beschaffung	Hiermit ist der Leiter der Beschaffungsstelle oder der Organisationseinheit gemeint, die für die Beschaffung zuständig ist.
Leiter Fachabteilung	Dies bezeichnet den Leiter einer Fachabteilung.
Leiter Haustechnik	Hiermit ist der Verantwortliche für die Haustechnik gemeint.
Leiter Innerer Dienst	Dies bezeichnet den Leiter des Inneren Dienstes bzw. den Verantwortlichen für die Bereitstellung zentraler Dienste.
Leiter IT	Hiermit ist der Leiter der IT-Abteilung bzw. das für die Informationstechnik zuständige Management gemeint.
Leiter Organisation	Dies bezeichnet den Leiter der Organisationseinheit, die u. a. für Regelung und Überwachung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist.
Leiter Personal	Hiermit ist der Leiter der Personalabteilung bzw. der für Personalfragen zuständigen Organisationseinheit gemeint.
Mitarbeiter	Ein Mitarbeiter ist Mitglied einer Fachabteilung, einer Behörde oder eines Unternehmens.
Netzadministrator	Ein Netzadministrator ist zuständig für Einrichtung, Betrieb, Kontrolle der Nutzung und Wartung eines Computernetzes oder -teilnetzes. Zu seinen Aufgaben gehört beispielsweise die Erstellung eines Netzplans, die Einrichtung neuer Dienste und die Auswertung von Protokolldateien.
Netzplaner	Ein Netzplaner ist verantwortlich für die Planung der Struktur der IT-Netze und der Anbindungen an externe und öffentliche Netze.
Notfall-Verantwortliche	Der Notfall-Verantwortliche ist von der Behörden- bzw. Unternehmensleitung autorisiert darüber zu entscheiden, ob es sich bei einer bestimmten Situation um einen Notfall handelt, und ggf. für die Einleitung erforderlicher Notfallmaßnahmen verantwortlich.
Personalabteilung	Die Personalabteilung ist u. a. für folgende Aufgaben zuständig: <ul style="list-style-type: none"> <li>- Personalwirtschaftliche Grundfragen</li> <li>- Personalbedarfsplanung</li> <li>- Personalbeschaffung</li> <li>- Personaleinsatz</li> <li>- Personalangelegenheiten der Mitarbeiter</li> <li>- Soziale Betreuung der Mitarbeiter</li> <li>- Allgemeine Zusammenarbeit mit der Personalvertretung</li> </ul>

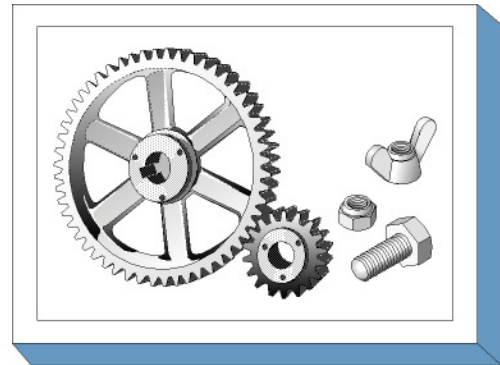
Personalrat/Betriebsrat	Der Personal- bzw. Betriebsrat ist für die Interessenvertretung der Mitarbeiter gegenüber der Behörden- bzw. Unternehmensleitung zuständig.
Planer	Einführung des allgemeinen Begriffs "Planer" anstatt der Begriffe "Netzplaner" und "Bauplaner".
Poststelle	Die Poststelle ist die Sammelstelle einer Behörde oder eines Unternehmens für ankommende und ausgehende Post. Zu ihren Aufgabengebieten können auch Fax- und E-Maildienstleistungen gehören.
Pressestelle	Die Pressestelle ist zuständig für alle ein- und ausgehenden Kontakte zu Presse und Medien.
Revisor	Ein Revisor kontrolliert, ob die geplanten Maßnahmen adäquat umgesetzt wurden.
Telearbeiter	Ein Telearbeiter verrichtet im allgemeinen Tätigkeiten, die räumlich entfernt vom Standort des Arbeit- bzw. Auftraggebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers unterstützt wird.
TK-Anlagen-Verantwortlicher	Der TK-Anlagen-Verantwortliche ist für den Betrieb der Telekommunikationsanlagen und für entsprechende Regelungen verantwortlich.
Verantwortliche der einzelnen IT-Anwendungen	Der Verantwortliche für die einzelne IT-Anwendung ist nicht nur zuständig für den reibungslosen Betrieb der IT-Anwendung, sondern auch für die Initiierung und Umsetzung von IT-Sicherheitsmaßnahmen für diese Anwendung.
Verantwortliche für die Datensicherung	Der Verantwortliche für die Datensicherung ist zuständig für die Erstellung, Pflege, regelmäßige Aktualisierung und Umsetzung eines Datensicherungskonzeptes.
Vorgesetzte	Als Vorgesetzte werden die Mitglieder der Institution bezeichnet, die gegenüber der betrachteten Position weisungsbefugt sind.

## 4 Glossar und Begriffsdefinitionen

In diesem Glossar werden einige wichtige Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert.

### Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.



### Application-Level-Gateway (ALG)

Ein Application-Level-Gateway ist ein IT-System, das die Informationen der Anwendungsschicht (das heißt, den tatsächlichen Inhalt (die Nutzdaten) eines Paketes oder mehrerer zusammengehöriger Pakete) filtert und anhand spezieller Regeln Verbindungen oder auch bestimmte Kommandos verbieten oder erlauben kann. Ein Application-Level-Gateway ist im Allgemeinen auf einem IT-System implementiert, das ausschließlich für diese Aufgabe eingesetzt wird und dessen Befehlsumfang auf das Notwendigste reduziert ist.

### Authentisierung

Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird.

### Authentikation (häufig auch Authentifikation, englisch authentication)

Authentikation bezeichnet den Nachweis der Identität gegenüber einem Kommunikationspartner. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

### Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

### Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

### Basis-Sicherheitscheck

Der Begriff bezeichnet gemäß IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Maßnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden IT-Sicherheitsmaßnahmen noch fehlen.

### Baustein

Der Begriff dient im IT-Grundschutz zur Strukturierung von Informationstechnik und ihrer Einsatzumgebung. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie

Notfallvorsorge-Konzept) und besondere Einsatzformen (wie Häuslicher Arbeitsplatz). In jedem Baustein werden die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

**Bedrohung (threat)**

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht. Bedrohungen können sich aus Einwirkungen durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen ergeben.

**Benutzerkennung (häufig auch Benutzerkonto)**

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine automatisch vergebene Kombination aus Buchstaben oder Ziffern.

**Blackbox-Test**

Bei Blackbox-Tests wird das Verhalten von Außentätern simuliert, wobei vorausgesetzt wird, dass der Angreifer keine oder nur oberflächliche Informationen über sein Angriffsziel hat.

**Browser**

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

**Client**

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

**Computer-Virus**

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

**Datenschutz**

Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

**Datensicherheit**

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist "IT-Sicherheit".

**Datensicherung (englisch: Backup)**

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt.



Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustandes von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

### **Demilitarisierte Zone (DMZ)**

Eine DMZ ist ein Zwischennetz, das am Übergang zwischen dem Intranet und dem Internet platziert wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das Intranet.

DMZ werden bei einfachen Sicherheit Gateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt (die anderen beiden Schnittstellen sind mit dem Intranet bzw. Internet verbunden). Besteht das Sicherheit Gateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

### **Digitale Signatur**

Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

### **Ergänzende Sicherheitsanalyse**

Diese Analyse ist nach IT-Grundschutz bei hohem Schutzbedarf oder zusätzlichem Analysebedarf durchzuführen, um gegebenenfalls zusätzliche oder höherwertige IT-Sicherheitsmaßnahmen festzulegen. Die Vorgehensweise ist im Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschrieben.

### **Gefahr**

"Gefahr" wird oft als übergeordneter Begriff gesehen, wohingegen unter "Gefährdung" eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. Die Gefährdungen sind dann "defekter Datenträger" und "Diebstahl von Datenträgern". Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, "Gefahr" und "Gefährdung" als gleichbedeutend aufzufassen.

### **Gefährdung**

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenverseuchte Datei



herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Computer-Viren-Typ ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

### **Gefährdungskataloge**

Teil der IT-Grundschatz-Kataloge: In die Schadensursachen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen sortierte Kataloge mit Beschreibungen möglicher Gefährdungen der Informationstechnik.

### **Grundwerte der IT-Sicherheit**

Der IT-Grundschatz betrachtet die drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der IT-Sicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit

### **Informationstechnik (IT)**

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

### **Infrastruktur**

Beim IT-Grundschatz werden unter Infrastruktur die für IT genutzten Gebäude und Räume verstanden. Die IT-Systeme gehören nicht dazu.

### **Integrität**

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

### **Intranet**

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netze (wie dem Internet) durch eine Firewall abgesichert.

### **IT-Grundschatz**

IT-Grundschatz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von IT-Verbänden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-

Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen für IT-Systeme mit normalem Schutzbedarf umgesetzt sind. Für Systeme mit hohem oder sehr hohem Schutzbedarf sind möglicherweise darüber hinausgehende Sicherheitsmaßnahmen notwendig.

### **IT-Grundschutzanalyse**

Zu einer IT-Grundschutzanalyse gehören die Modellierung mit der Ermittlung der notwendigen Sicherheitsmaßnahmen und der Basis-Sicherheitscheck, in dem ein Soll-Ist-Vergleich den aktuellen Umsetzungsgrad von Sicherheitsmaßnahmen in einem Unternehmen oder einer Behörde beschreibt.

### **IT-Grundschutz-Zertifizierung (auch IT-Grundschutz-Qualifizierung)**

Verfahren, in dem Unternehmen oder Behörden ihre (gemäß IT-Grundschutz) erreichten IT-Sicherheitsniveaus überprüfen lassen. Ein vom BSI lizenzierter IT-Grundschutz-Auditor führt die Überprüfung durch und erstellt einen Auditreport. Die Zertifizierungsstelle BSI stellt aufgrund des Auditreports fest, ob die notwendigen IT-Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein IT-Grundschutz-Zertifikat und veröffentlicht es.

### **IT-Sicherheit**

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

Es gibt drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der IT-Sicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit

### **IT-Sicherheitsbeauftragter**

Person mit eigener Fachkompetenz zur IT-Sicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, der für alle IT-Sicherheitsfragen, Mitwirkung im IT-Sicherheitsprozess und IT-Sicherheitsmanagement-Team zuständig ist, die IT-Sicherheitsleitlinie, das IT-Sicherheitskonzept und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellt und deren Umsetzung plant und überprüft.

### **IT-Sicherheitskonzept**

Ein IT-Sicherheitskonzept dient zur Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

### **IT-Sicherheitskonzeption**

Die Erstellung einer IT-Sicherheitskonzeption ist eine der zentralen Aufgaben des IT-Sicherheitsmanagements. Aufbauend auf den Ergebnissen von IT-Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen IT-Sicherheitsmaßnahmen identifiziert und im IT-Sicherheitskonzept dokumentiert.

**IT-Strukturanalyse**

In einer IT-Strukturanalyse werden die erforderlichen Informationen über den ausgewählten IT-Verbund, die IT-Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

**IT-Verbund**

Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

**Kumulationseffekt**

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensibler Informationen auf einem IT-System verarbeitet werden, so dass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

**Maßnahmenkatalog**

In den IT-Grundschutz-Katalogen werden zu jedem Baustein passende Maßnahmen empfohlen. Diese sind in Katalogen zusammengefasst, die in Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge gegliedert sind.

**Maximum-Prinzip**

Nach dem Maximum-Prinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

**Modellierung**

Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete IT-Verbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen nachgebildet.

**Netzplan**

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

**Nichtabstreitbarkeit (non repudiation):**

Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

**Paketfilter**

Paketfilter sind IT-Systeme mit spezieller Software, die die Informationen anhand der Header-Daten der unteren Schichten (Transportschicht oder Verbindungsschicht) des OSI-Modells filtern und anhand spezieller Regeln Pakete weiterleiten oder verwerfen. Paketfilter treffen ihre Entscheidungen beispielsweise anhand von Quell- und Ziel-Adressen oder -Ports eines Paketes, ohne den Inhalt zu berücksichtigen.

**Patch**

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

**Penetrationstest**

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

**Proxy**

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

**Qualifizierungsstufe (auch Siegel- oder Zertifikatsstufe)**

Die IT-Grundschutz-Methodik sieht drei Qualifizierungsstufen vor: "A" für die IT-Grundschutz-Einstiegsstufe, "B" für die IT-Grundschutz-Aufbaustufe, "C" für das IT-Grundschutz-Zertifikat. Mit "Z" werden Maßnahmen bezeichnet, die Ergänzungen darstellen, die vor allem bei höheren Sicherheitsanforderungen erforderlich sein können.

**Revision**

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-) Richtlinien. Die Revision sollte unabhängig und neutral sein.

**Risiko**

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

**Risikoanalyse (englisch Risk Assessment/Analysis)**

Mit einer Risikoanalyse wird untersucht, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen der Schaden hätte.

**Schadfunktion**

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Verfügbarkeit von Daten, Ressourcen oder Dienstleistungen, die Vertraulichkeit von Daten oder die Integrität von Daten unbeabsichtigt oder bewusst gesteuert gefährden kann.

**Schutzbedarf**

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

**Schutzbedarfsdefinitionen**

Auf die jeweils betrachtete Institution angepasste Kriterien, anhand derer entschieden werden kann, welche Schutzbedarfskategorie auf eine IT-Komponente anzuwenden ist.

**Schutzbedarfsfeststellung**

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

**Schwachstelle (vulnerability)**

Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

**Server**

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder Mail-Server. Zu häufiger Verwirrung führen X-Server, da ein X-Server-Prozess typischerweise auf einem Arbeitsplatzrechner, also einem Client in einem Server-Client-Netz, läuft.

**Sicherheitskonzept**

In einem Sicherheitskonzept werden die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben.

**Sicherheitsmaßnahme**

Mit Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung, oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde "safeguard" gewählt. Im englischen Sprachraum wird neben "safeguard" häufig der Begriff "control" verwendet.

**Sicherheitsrichtlinie (englisch Security Policy)**

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

**Sicherheitspolitik**

Falsche Übersetzung von Security Policy, siehe Sicherheitsrichtlinie

**Standardsoftware**

Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

**Trojanisches Pferd**

Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung.

**Verbindlichkeit**

Unter Verbindlichkeit werden die IT-Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

**Verfügbarkeit**

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen.

**Verschlüsselung**

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffre), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

**Verteilungseffekt**

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine IT-Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der IT-Anwendung laufen.

**Vertraulichkeit**

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

**Wert (asset)**

Alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

**Zertifikat**

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

- IT-Grundsatz-Zertifikat: Da das Vorgehen nach IT-Grundsatz zusammen mit den IT-Grundsatz-Katalogen ein anerkanntes Kriterienwerk für IT-Sicherheit darstellt, hat das BSI ein Zertifizierungsschema für IT-Grundsatz erarbeitet. Damit kann durch ein IT-Grundsatz-Zertifikat dokumentiert werden, dass für den betrachteten IT-Verbund alle relevanten Sicherheitsmaßnahmen aus den IT-Grundsatz-Katalogen realisiert wurden.
- Zertifikat (Schlüsselzertifikat): Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfchlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehört.
- Zertifikat (IT-Sicherheitszertifikat, CC-Zertifikat): Zertifiziert wird nach international anerkannten IT-Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser können Produkte und Systeme unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung

ist jedoch, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen.

- Zertifikat von Schutzprofilen (Profil-Zertifikate): Mit Schutzprofilen wird bei den Common Criteria Anwendergruppen und Herstellern die Möglichkeit gegeben, produktklassentypische und dienstleistungsspezifische Sicherheitsanforderungen festzulegen. Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den anwenderspezifischen Anforderungen entsprechen. Auch Schutzprofile können evaluiert und zertifiziert werden.